

Amdt. dated June 7, 2004
Reply to Office action of 03/05/2004

Serial No. 09/409,633
Docket No. BO999025
Firm No. 0036.0039

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

1. (Currently amended) A method for accessing a control system in a server from a client computer, wherein the control system includes a logon program to enable the client computer to use a terminal emulation program to logon to the server to access a client process executing in the server to perform control system operations, further comprising:

requesting, with the client, a security context for the client including authorization to allow the client to access control system functions in the server, wherein the security context is associated with a client credential information including access for which the client is authorized; ~~and wherein the server is capable of impersonating the client to generate the security context;~~

impersonating the client, by the server, to generate the security context;

returning, with the server, the generated requested security context to the client; and

transmitting, with a client program executing in the client, a control system command and the security context to access the control system in the server; and

based on the control system command, reconfiguring a printer object, wherein the requesting, the impersonating, the returning, the transmitting, and the reconfiguring are performed without using the logon program to enable the client to logon to the server.

2. (Previously presented) The method of claim 1, wherein requesting with the client comprises the client requesting the server to impersonate the client to obtain the security context, further comprising accessing, with the server impersonating the client, the security context to return to the client.

3. (Original) The method of claim 2, wherein the Distributed Computing Environment (DCE) protocol is used to provide the client security context, wherein the client uses the sec_login_become_initiator DCE command to request the server to impersonate the client,

Arodt, dated June 7, 2004
Reply to Office action of 03/05/2004

Serial No. 09/409,633
Docket No. BO999025
Firm No. 0036.0039

wherein the server uses the `sec_login_become_impersonator` DCE command to impersonate the client to obtain the security context.

4. (Original) The method of claim 1, further comprising:
converting, with the server, the security context transmitted through the client program to a pointer to credential information of the client;
determining from the credential information, with the server, whether the client is authorized to invoke the transmitted control system command; and
executing, with the server, the control system command transmitted by the client if the client is authorized to invoke the command.

5. (Original) The method of claim 1, wherein the client computer includes a different operating system than the server, wherein the client program executing in the client interacts with the client process executing in the server to perform control system operations.

6. (Original) The method of claim 1, wherein the client requests the security context through a remote procedure call.

7. (Original) The method of claim 1, wherein the control system is a printing systems manager to control printers and printer related objects managed by the server.

8. (Original) The method of claim 7, wherein the printer system manager command transmitted by the client comprises a command to reconfigure at least one printer object, thereby allowing the client computer to perform administrative functions.

9. (Currently amended) A system for accessing a control system in a server from a client computer, wherein the control system includes a logon program to enable the client

Amdt. dated June 7, 2004
Reply to Office action of 03/05/2004

Serial No. 09/409,633
Docket No. BO999025
Firm No. 0036.0039

computer to use a terminal emulation program to logon to the server to access a client process
executing in the server to perform control system operations, further comprising:

means for requesting a security context for the client including authorization to allow the
client to access control system functions in the server, wherein the security context is associated
with a client credential information including access for which the client is authorized; and
~~wherein the server is capable of impersonating the client to generate the security context;~~

means for impersonating the client, by the server, to generate the security context;

means for returning the requested generated security context to the client; and

means for transmitting with a client program executing in the client a control system
command and the security context to access the control system in the server; and

means for reconfiguring a printer object, wherein the requesting, the impersonating, the
returning, the transmitting, and the reconfiguring are performed without using the logon program
to enable the client to logon to the server, and wherein reconfiguration of the at least one printer
object is based on the control system command.

10. (Previously presented) The system of claim 9, wherein the means for requesting the
security context comprises the server impersonating the client to obtain the security context,
further comprising means for accessing, with the server impersonating the client, the security
context to return to the client.

11. (Original) The system of claim 10, wherein the Distributed Computing Environment
(DCE) protocol is used to provide the client security context, wherein the client uses the
sec_login_become_initiator DCE command to request the server to impersonate the client,
wherein the server uses the sec_login_become_impersonator DCE command to impersonate the
client to obtain the security context.

12. (Original) The system of claim 9, further comprising:

Amdt. dated June 7, 2004
Reply to Office action of 03/05/2004

Serial No. 09/409,633
Docket No. BO999025
Firm No. 0036.0039

means for converting the security context transmitted through the client interface to a pointer to credential information of the client;
means for determining from the credential information whether the client is authorized to invoke the transmitted control system command; and
means for executing the control system command transmitted by the client if the client is authorized to invoke the command.

13. (Original) The system of claim 9, wherein the client computer includes a different operating system than the server, wherein the client program is part of the client operating system, and wherein the client program interacts with the client process executing in the server to perform control system operations.

14. (Original) The system of claim 9, wherein the client requests the security context through a remote procedure call.

15. (Original) The system of claim 9, wherein the control system is a printing systems manager to control printers and printer related objects managed by the server.

16. (Original) The system of claim 15, wherein the printer system manager command transmitted by the client comprises a command to reconfigure at least one printer object, thereby allowing the client computer to perform administrative functions.

17. (Currently amended) An article of manufacture for use in accessing a control system in a server from a client computer, wherein the control system includes a logon program to enable the client computer to use a terminal emulation program to logon to the server to access a client process executing in the server to perform control system operations, the article of

Amdt. dated June 7, 2004
Reply to Office action of 03/05/2004

Serial No. 09/409,633
Docket No. BO999025
Firm No. 0036.0039

manufacture comprising computer usable media including computer programs embedded therein that cause the client and server computer to perform:

requesting, with the client, a security context for the client including authorization to allow the client to access control system functions in the server, wherein the security context is associated with a client credential information including access for which the client is authorized; and wherein the server is capable of impersonating the client to generate the security context;

impersonating the client, by the server, to generate the security context;

returning, with the server, the requested generated security context to the client; and

transmitting, with a client program executing in the client, a control system command and the security context to access the control system in the server; and

based on the control system command, reconfiguring a printer object, wherein the requesting, the impersonating, the returning, the transmitting, and the reconfiguring are performed without using the logon program to enable the client to logon to the server.

18. (Previously presented) The article of manufacture of claim 17, wherein requesting the security context comprises the client requesting the server to impersonate the client to obtain the security context, further comprising accessing, with the server impersonating the client, the security context to return to the client.

19. (Original) The article of manufacture of claim 18, wherein the Distributed Computing Environment (DCE) protocol is used to provide the client security context, wherein the client uses the sec_login_become_initiator DCE command to request the server to impersonate the client, wherein the server uses the sec_login_become_impersonator DCE command to impersonate the client to obtain the security context.

20. (Original) The article of manufacture of claim 17, further causing the server to perform:

Amdt. dated June 7, 2004
Reply to Office action of 03/05/2004

Serial No. 09/409,633
Docket No. B0999025
Firm No. 0036.0039

converting the security context transmitted through the client program to a pointer to credential information of the client;
determining from the credential information whether the client is authorized to invoke the transmitted control system command; and
executing the control system command transmitted by the client if the client is authorized to invoke the command.

21. (Original) The article of manufacture of claim 17, wherein the client computer includes a different operating system than the server, wherein the client program executing in the client interacts with the client process executing in the server to perform control system operations.

22. (Original) The article of manufacture of claim 17, wherein the client requests the security context through a remote procedure call.

23. (Original) The article of manufacture of claim 17, wherein the control system is a printing systems manager to control printers and printer related objects managed by the server.

24. (Original) The article of manufacture of claim 23, wherein the printer system manager command transmitted by the client comprises a command to reconfigure at least one printer object, thereby allowing the client computer to perform administrative functions.

25. (New) The method of claim 1, wherein the server comprises a printer manager executing in a first operating system, wherein the first operating system is different from a second operating system executing in the client, wherein the printer manager is implemented in a printer management server software, wherein the client accesses the printer manager to perform printer management and configuration operations including deleting, modifying, and creating

Amdt. dated June 7, 2004
Reply to Office action of 03/05/2004

Serial No. 09/409,633
Docket No. BO999025
Firm No. 0036.0039

printer objects, and submitting print jobs, and wherein the printer manager impersonates the client to generate the security context.

26. (New) The method of claim 25, wherein an user on the client does not have to logon onto the printer manager by using an existing login facility, and wherein the client sends the security context to the printer manager with a print command in a language of the printer manager.

27. (New) The system of claim 9, wherein the server comprises a printer manager executing in a first operating system, wherein the first operating system is different from a second operating system executing in the client, wherein the printer manager is implemented in a printer management server software, wherein the client accesses the printer manager to perform printer management and configuration operations including deleting, modifying, and creating printer objects, and submitting print jobs, and wherein the printer manager impersonates the client to generate the security context.

28. (New) The system of claim 27, wherein an user on the client does not have to logon onto the printer manager by using an existing login facility, and wherein the client sends the security context to the printer manager with a print command in a language of the printer manager.

29. (New) The article of manufacture of claim 17, wherein the server comprises a printer manager executing in a first operating system, wherein the first operating system is different from a second operating system executing in the client, wherein the printer manager is implemented in a printer management server software, wherein the client accesses the printer manager to perform printer management and configuration operations including deleting, modifying, and

Amtd. dated June 7, 2004
Reply to Office action of 03/05/2004

Serial No. 09/409,633
Docket No. BO999025
Exam No. 0036.0039

creating printer objects, and submitting print jobs, and wherein the printer manager impersonates the client to generate the security context.

30. (New) The article of manufacture of claim 29, wherein an user on the client does not have to logon onto the printer manager by using an existing login facility, and wherein the client sends the security context to the printer manager with a print command in a language of the printer manager.